UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/890,180	01/24/2002	Alexander Medvinsky	D02236-02	7559

43471 7590 01/23/2009
Motorola, Inc.
Law Department
1303 East Algonquin Road
3rd Floor
Schaumburg, IL 60196

EXAMINER	
TO, BAOTRAN N	
ART UNIT	PAPER NUMBER
2435	
NOTIFICATION DATE	DELIVERY MODE
01/23/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

Docketing.US@motorola.com

Office Action Summary	Application No.	Applicant(s)	
	09/890,180	MEDVINSKY ET AL.	
	Examiner	**Art Unit**	
	Baotran N. To	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _05 November 2008_.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-19_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-19_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1. This Office action is responsive to the Applicant's Amendment filed 11/05/2008.

Claims 1, 6, 7, 11, and 15 are amended.

Claims 1-19 are presented for examination.

Response to Arguments

2. Applicant's arguments filed 11/05/2008 have been fully considered but they are not persuasive.

Applicant appears to argue that "The Barkan and Ganesan references, taken either alone or in combination, do not describe a communications path from the first telephony adapter to the second telephone adapter is routed through the first and second gateway controllers" (Page 10 of Remarks).

This argument is not persuasive because Barkan clearly discloses the above limitation in Figure 1, communication path from communication channel 103 of facility 1 to communication channel 107 of facility 2 is routed through key distribution center 11 and key distribution center 12. Furthermore, Barkan discloses for example, Figure 1 details a system implementation using separate channels for key distribution (103) and for communications with another user (213); a different implement may **use the same channel for both purpose** (col. 14, lines 11-15).

Applicant appears to argue that "The Barkan and Ganesan references, taken either alone or in combination, do not describe generating a secret key at first gateway controller, distributing the secret key to the first and second telephony adapters over previously established secure connections and establishing the secure communication channel between the first user and the second user by encrypting and decrypting information using the secret key" (Page 11 of Remarks).

The above argument is not persuasive because Ganesan clearly discloses the above limitations in figure 2 such as “In step 210 a request is received from a user using user station 30 to establish a communication session with a user at user station 32. The request is transmitted via the network to processor 50. In response to the request, **processor 50 generates a session key** in step 212……… Now that **a session key has been distributed, communications between user stations 30 and 32** can be secured. Thus, in step 218 a message is generated on station 30. **The message is encrypted in step 220 by the station 30 processor with the session key. The encrypted message is transmitted via the network to station 32 and decrypted by the station 32 processor using the session key received by station 32**” (col. 9, line 26 –57).

In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

For at least the above reasons, the rejections for Claims 1-19 are maintained.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Barkan (EP 0738085 A2) herein referred to as Barkan in view of Ganesan (U.S. Patent 5,838,792) herein referred to as Ganesan.

Regarding on Claims 1 and 6, Barkan discloses a method for establishing a secure communication channel in an IP telephony network between a first and a second user, wherein the first user and the second user are coupled to first and second telephony adapters, which in turn, are coupled to first and second gateway controllers, respectively, wherein the gateway controllers control user access to the IP telephony network, and wherein the telephony adapters encrypt and decrypt user information exchanged over the IP telephony network (Fig. 1), the method comprising:

receiving a request at the first gateway controller (key distribution center 11) to establish a secure communication channel (secure communication link) between the first user (facility 1) and the second user (facility 3) (Fig. 1, col. 3, lines 17-25 and col. 4, lines 1-2); generating keys at the gateway controller (col. 8, lines 29-34, i.e., the user can go to a cellular phone company center to compute there and loads new keys, for example by connecting to terminals in that center).

Barkan does not disclose generating a secret key at the first gateway controller; distributing the secret key to the first and second telephony adapters over previously established secure connections; and establishing the secure communication channel between the first user and the second user by encrypting and decrypting information using the secret key.

However, Ganesan explicitly discloses generating a secret key (session key) at the first gateway controller (Figure 1, element 50, Figure 2, element 212 col. 3, line 65 - col. 4, line 1 and col. 9, line 26 –57); distributing the secret key to the first and second telephony adapters over previously established secure connections (Figure 1, elements 30 and 32, col. 9, lines 50-52); and establishing the secure communication channel between the first user and the second user by encrypting and decrypting information using the secret key (Figure 2, elements 218 and 220, col. 9, lines 50-57).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have combined Ganesan's invention with Barkan to include generating a secret key at the first gateway controller; distributing the secret key to the first and second telephony adapters over previously established secure connections; and establishing the secure communication channel between the first user and the second user by encrypting and decrypting information using the secret key. One of ordinary skill in the art would have been motivated to do so because it would provide secure communications during a communication session between users as taught by Ganesan (Abstract).

Barkan and Ganesan disclose the limitations of Claims 1 and 6 above. Barkan and Ganesan further disclose wherein communications between the first telephony adapter and the second telephony adapter are routed through the first gateway controller and the second gateway controller (Barkan, Figure 1, communication channel channels 103, 111, and 107 between facility 1 and facility 3 are go through key distribution center 11 and key distribution center 12, col. 14, lines 11-15).

Regarding on Claim 2, Barkan and Ganesan disclose the limitations as discussed in Claim 1 above. Barkan further discloses wherein the step of generating comprises a step of generating a random number at the first gateway controller to be used as the secret key (col. 14, line 59 and col. 15, lines 1-5).

Regarding on Claim 3, Barkan and Ganesan disclose the limitations as discussed in Claim 1 above. Barkan further discloses wherein the step of generating comprises a step of deriving the secret key at the first gateway controller (col. 15, lines 5-10), wherein the secret key is derived from a signaling key shared between the first telephony adapter and the first gateway controller (col. 15, lines 15-20).

Regarding on Claim 4, Barkan and Ganesan disclose the limitations as discussed in Claim 1 above. Barkan further discloses transmitting the secret key from the first gateway controller to the second gateway controller (col. 7, lines 45-55); transmitting the secret key from the second gateway controller to the second telephony adapter (col. 7, lines 45-50), transmitting the secret key from the first gateway controller to the first telephony adapter (col. 6, lines 35-40).

Regarding on Claim 5, Barkan and Ganesan disclose the limitations as discussed in Claim 1 above. Ganesan further discloses receiving a request at the first gateway controller to provide the secret key to a law enforcement server; and providing the secret key to the law enforcement server (col. 4, lines 16-62).

Regarding on Claim 7, Barkan discloses a gateway controller for establishing a secure communication channel in an IP telephony network, the gateway controller coupled between a telephony adapter and a telephony network backbone (Fig. 1), the gateway controller (key distribution center) comprising:

a key storage module (key management controller) coupled to the key creation module and having logic to store the secret key (col. 8, lines 15-20); and

a message processor coupled to the key creation module and the key storage module (col. 8, lines 15-20), and having logic to process messages exchanged between the telephony adapter and the telephony network backbone (Fig. 1, element 111) (col. 7, lines 51-54 and col. 14, lines 15-30), wherein the message processor further comprises:

logic to receive a request to establish a secure communication channel between a first user and a second users the first user couple to the telephony adapter, the second user coupled to a remote telephony adapter (Fig. 1, col. 3, lines 17-25 and col. 4, lines 1-2); create keys at the gateway controller (col. 8, lines 29-34, i.e., the user can go to a cellular phone company center to compute there and loads new keys, for example by connecting to terminals in that center).

Barkan explicitly does not disclose a key creation module having logic to create a secret key; logic to distributed the secret key to the telephony adapters over previously established secure connections, whereby the secure communication channel between the first user and the second user may be established by encrypting and decrypting information using the secret key.

However, Ganesan explicitly discloses a key creation module having logic to create a secret key (session key) (Figure 1, element 50, Figure 2, element 212 col. 3, line 65 - col. 4, line 1); logic to distributed the secret key to the telephony adapters over previously established secure connections over previously established secure connections (Figure 1, elements 30 and 32, col. 9, lines 50-52); and whereby the secure communication channel between the first user and the second user may be established by encrypting and decrypting information using the secret key (Figure 2, elements 218 and 220, col. 9, lines 50-57).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have combined Ganesan's invention with Barkan to include a key creation module having logic to create a secret key; logic to distributed the secret key to the telephony adapters over previously established secure connections; whereby the secure communication channel between the first user and the second user may be established by encrypting and decrypting information using the secret key. One of ordinary skill in the art would have been motivated to do so because it would provide secure communications during a communication session between users as taught by Ganesan (Abstract).

Barkan and Ganesan disclose the limitations of Claim 7. Barkan and Ganesan further disclose wherein communications between the first telephony adapter and the second telephony adapter are routed through the first gateway controller and the second gateway controller (Barkan, Figure 1, communications between facility 1 and facility 3 are go through key distribution center 11 and key distribution center 12, col. 14, lines 11-15).

Regarding on Claim 8, Barkan and Ganesan disclose the limitations as discussed in Claim 7 above. Barkan further discloses wherein the key creation module has logic to generate a random number as the secret key (col. 14, line 59 and col. 15, lines 1-5).

Regarding on Claim 9, Barkan and Ganesan disclose the limitations as discussed in Claim 7 above. Barkan further discloses wherein the key creation module has logic to derive the secret key from a signaling key shared with the telephony adapter (col. 8, lines 15-40).

Regarding on Claim 10, Barkan and Ganesan disclose the limitations as discussed in Claim 7 above. Barkan and Ganesan further disclose wherein the key storage module has logic to encrypt the secret key before storage (Barkan, col. 10, lines 20-25) using a public/private key pair belonging to law enforcement (Ganesan, col. 4, lines 16-62).

Regarding on Claim 11, Barkan discloses a system for providing encrypted communications in an IP telephony network, said system comprising:

a first cable telephony adapter (facility 1 key management device) (col. 5, lines 53-55);

a first gateway controller (key distribution center 11) coupled with said first cable telephony adapter (col. 6, lines 25-30);

a second cable telephony adapter (facility 3 key management device) (col. 5, lines 52-55);

a second gateway controller (key distribution center 12) coupled with said second cable telephony adapter (col. 7, lines 45-50);

a network coupled with both said first gateway controller and said second gateway controller so as to facilitate communications between said first cable telephony adapter and said second cable telephony adapter wherein said communications between said first cable telephony adapter and said second cable telephony adapter are routed said first gateway controller and said second gateway controller (communications between facility 1 and facility 3 are go through key distribution center 11 and key distribution center 12, Fig. 1, col. 14, lines 11-15).

Barkan explicitly does not disclose wherein said first gateway controller comprises: a first key creation module configured to generate a secret key for distribution to both said first cable telephony adapter and said second cable telephony adapter for use in encrypted communications between said first cable telephony adapter and said second cable telephony adapter.

However, Ganesan explicitly discloses wherein said first gateway controller comprises: a first key creation module configured to generate a secret key (session key) for distribution to both said first cable telephony adapter and said second cable telephony adapter for use in encrypted communications between said first cable telephony adapter and said second cable telephony adapter over previously established secure connections (Figure 1, elements 30, 32, and 50, col. 9, lines 26-57).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have combined Ganesan's invention with Barkan to include wherein said first gateway controller comprises: a first key creation module configured to generate a secret key for distribution to both said first cable telephony adapter and said second cable telephony adapter for use in encrypted communications between said first cable telephony adapter and said second cable telephony adapter. One of ordinary skill in the art would have been motivated to do so because it would provide secure communications during a communication session between users as taught by Ganesan (Abstract).

Regarding on Claim 12, Barkan and Ganesan disclose the limitations as discussed in Claim 11 above wherein said second gateway controller comprises:

a second key creation module configured to generate a secret key for distribution to both said first cable telephony adapter and said second cable telephony adapter for use in encrypted communications between said first cable telephony adapter and said second cable telephony adapter (col. 8, lines 30-35 and Abstract, lines 1-5).

Regarding on Claim 13, Barkan and Ganesan disclose the limitations as discussed in Claim 11 above wherein said first gateway controller further comprises:

a message processor configured to receive an encrypted message from said first cable telephony adapter intended for decryption by said second cable telephony adapter and further configured to forward said encrypted message to said second gateway controller without decrypting said encrypted message (col. 7, lines 51-54 and col. 14, lines 15-30).

Regarding on Claim 14, Barkan and Ganesan disclose the limitations as discussed in Claim 7 above. Barkan further discloses wherein said key creation module is configured to intermittently generate a second secret key and to distribute said second secret key to said first cable telephony adapter and said second cable telephony adapter so as to replace said previously generated secret key (col. 7, lines 45-59 and col. 8, lines 1-40).

Regarding on Claim 15, Barkan discloses a method of establishing secure communications between a first cable telephony adapter and a second cable telephony adapter in a system in which secure communications do not previously exist between said first cable telephony adapter and said second cable telephony adapter, wherein said first cable telephony adapter is coupled with a first gateway controller, said second cable telephony adapter is coupled with a second gateway controller, and a network is coupled with said first gateway controller and said second gateway controller (Fig. 1), said method comprising:

receiving at said first gateway controller (key distribution center 11) a request from said first cable telephony adapter to establish communications between said first cable telephony adapter (facility 1 key management device) and said second cable telephony adapter (facility 3 key management device) (Fig. 1, col. 3, lines 17-25 and col. 4, lines 1-2);

Barkan does not disclose "generating a secret key at said first gateway controller; distributing said secret key from said first gateway controller to said first cable telephony adapter."

However, Ganesan explicitly discloses generating a secret key (session key) at the first gateway controller (Figure 1, element 50, Figure 2, element 212 col. 3, line 65 - col. 4, line 1) and distributing said secret key from said first gateway controller to said first cable telephony adapter over previously established secure connections (col. 9, lines 50-52).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have combined Ganesan's invention with Barkan to include generating a secret key at said first gateway controller and distributing said secret key from said first gateway controller to said first cable telephony adapter. One of ordinary skill in the art would have been motivated to do so because it would provide secure communications during a communication session between users as taught by Ganesan (Abstract).

Barkan and Ganesan disclose the limitations of claims 15 above. Barkan and Ganesan further discloses distributing said secret key to said second gateway controller via a secure communication (Barkan, Figure 1, elements 11 and 12, and Ganesan, col. 9, lines 50-52); distributing said secret key from said second gateway controller to said second cable telephony adapter (Barkan, Figure 1, elements 11 and 12, and Ganesan, col. 9, lines 50-52),

wherein communications between the first telephony adapter and the second telephony adapter are routed through the first gateway controller and the second gateway controller (Barkan, Figure 1, communications between facility 1 and facility 3 are go through key distribution center 11 and key distribution center 12, col. 14, lines 11-15).

Regarding on Claim 16, Barkan and Ganesan disclose the limitations as discussed in Claim 15 above. Barkan further discloses encrypting a message at said first cable telephony adapter with said secret key (col. 6, lines 30-35); sending said encrypted message to said first gateway controller (col. 9, lines 45-50); receiving said encrypted message at said first gateway controller (col. 6, lines 25-40); forwarding said encrypted message from said first gateway controller to said second gateway controller without decrypting said encrypted message (col. 10, lines 45-55).

Regarding on Claim 17, Barkan and Ganesan disclose the limitations as discussed in Claim 15 above. Barkan further discloses receiving said encrypted message at said second gateway controller (col. 10, lines 45-50); forwarding said encrypted message from said second gateway controller to said second cable telephony adapter without decrypting said message (col. 10, lines 35-55); decrypting said encrypted message at said second cable telephony adapter (col. 15, lines 17-20).

Regarding on Claim 18, Barkan and Ganesan disclose the limitations as discussed in Claim 15 above. Barkan further discloses encrypting a message at said first cable telephony adapter with said secret key (col. 6, lines 30-35); sending said encrypted message to said first gateway controller (col. 9, lines 45-50); receiving said encrypted message at said first gateway controller (col. 6, lines 25-40); routing said encrypted message from said first gateway controller to said second cable telephony adapter (col. 12, lines 5-15).

Regarding on Claim 19, Barkan and Ganesan disclose the limitations as discussed in Claim 15 above. Barkan further discloses receiving said encrypted message at said second cable telephony adapter (col. 15, lines 15-17); decrypting said encrypted message at said second cable telephony adapter with said secret key (col. 15, lines 17-20).

Conclusion

4. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the

THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Baotran N. To whose telephone number is (571)272-8156. The examiner can normally be reached on Monday-Friday from 8:00 to 4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/B. N. T./
Examiner, Art Unit 2435
/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435